

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-198272

(43)公開日 平成10年(1998)7月31日

(51)Int.Cl.⁸
G 0 9 C 1/00
H 0 4 L 9/08

識別記号
6 3 0
6 4 0

F I
G 0 9 C 1/00 6 3 0 D
6 4 0 Z
H 0 4 L 9/00 6 0 1 D

審査請求 未請求 請求項の数10 O L (全 10 頁)

(21)出願番号 特願平8-351565

(22)出願日 平成8年(1996)12月27日

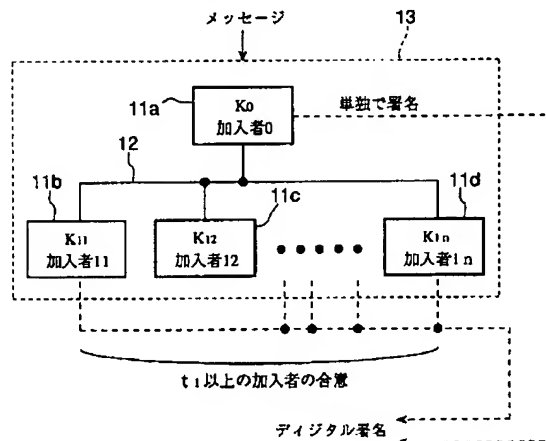
(71)出願人 000001007
キヤノン株式会社
東京都大田区下丸子3丁目30番2号
(72)発明者 長島 孝幸
東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内
(72)発明者 岩村 恵市
東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内
(74)代理人 弁理士 大塚 康德 (外1名)

(54)【発明の名称】 階層を有する鍵管理方法及び暗号システム、分散デジタル署名システム

(57)【要約】

【課題】 各加入者がデジタル署名生成などに関与できる度合いを階層的に管理することにより、階層構造を有するグループでの利用に適した鍵管理方法及び暗号システム、分散デジタル署名システムを提供する。

【解決手段】 通信路によって接続された複数の情報処理装置を含む情報通信システム上で機能する鍵管理方法において、秘密の鍵Kを保持する1個以上の第1の加入者11aと、元の秘密鍵Kを秘密分散することにより生成した部分情報 K_{1i} ($i=1, 2, \dots$) のうち1個以上を秘密に保持する複数の第2の加入者11b~11dとを設け、前記第1の加入者は自分の鍵Kを情報通信システムの鍵とすることができるのに対し、前記第2の加入者は所定数 t_1 以上の部分情報 K_{1i} を集めてはじめて情報通信システムの鍵とする。



Best Available Copy

【特許請求の範囲】

【請求項1】 通信路によって接続された複数の情報処理装置を含む情報通信システム上で機能する鍵管理方法において、

秘密の鍵 K を保持する1個以上の第1の加入者と、元の秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i = 1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の加入者とを設け、

前記第1の加入者は自分の鍵 K を情報通信システムの鍵とすることが出来るのに対し、前記第2の加入者は所定数以上の部分情報 K_{1i} を集めてはじめて情報通信システムの鍵とすることを特徴とする鍵管理方法。

【請求項2】 前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j = 1, 2, \dots$), K_{3ijm} ($m = 1, 2, \dots$), …のうちの1個以上を秘密に保持する複数の第3, 第4, …の加入者を設け、前記第3, 第4, …の加入者は、それぞれ所定数以上の部分情報 K_{2ij} , K_{3ijm} , …を集めてはじめて上層加入者の部分情報 K_{1i} , K_{2ij} , …とすることを特徴とする請求項1記載の鍵管理方法。

【請求項3】 元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上のついては、それらを保持する加入者を設けず、

最下層の部分情報については、それぞれを保持する全ての加入者を設けることを特徴とする請求項2記載の鍵管理方法。

【請求項4】 前記情報通信システムは、分散デジタル署名システム及び暗号システムのいずれかであることを特徴とする請求項1乃至3のいずれか1つに記載の鍵管理方法。

【請求項5】 通信路によって接続された複数の情報処理装置を含む分散デジタル署名システムであって、通信路によって接続された、秘密の鍵 K を保持する1個以上の第1の装置と、元の秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i = 1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の装置とを設け、前記第1の装置からは自分単独で署名をすることができるのに対し、前記第2の装置は所定数以上の合意があつてはじめて署名をすることができることを特徴とする分散デジタル署名システム。

【請求項6】 前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j = 1, 2, \dots$), K_{3ijm} ($m = 1, 2, \dots$), …のうちの1個以上を秘密に保持する複数の第3, 第4, …の装置を設け、前記第3, 第4, …の装置は、それぞれ所定数以上の合意があつてはじめて上層装置の意向となることを特徴とする請求項5記載の分散デジタル署名システム。

【請求項7】 元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上については、それらを保持する装置を設けず、

最下層の部分情報については、それぞれを保持する全ての装置を設けることを特徴とする請求項6記載の分散デジタル署名システム。

【請求項8】 通信路によって接続された複数の情報処理装置を含む暗号システムであって、

通信路によって接続された、秘密の鍵 K を保持する1個以上の第1の装置と、元に秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i = 1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の装置とを設け、前記第1の装置では自分単独で暗号化及び復号をすることができるのに対し、前記第2の装置は所定数以上の部分情報 K_{1i} を集めてはじめて暗号化及び復号をすることができることを特徴とする暗号システム。

【請求項9】 前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j = 1, 2, \dots$), K_{3ijm} ($m = 1, 2, \dots$), …のうちの1個以上を秘密に保持する複数の第3, 第4, …の装置を設け、前記第3, 第4, …の装置は、それぞれ所定数以上の部分情報 K_{2ij} , K_{3ijm} , …を集めてはじめて上層装置の部分情報 K_{1i} , K_{2ij} , …とすることを特徴とする請求項8記載の暗号システム。

【請求項10】 元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上については、それらを保持する装置を設けず、

最下層の部分情報については、それぞれを保持する全ての装置を設けることを特徴とする請求項9記載の暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信路で接続された複数の情報処理装置を有する環境を利用して、グループとして暗号やデジタル署名(認証)を扱う鍵管理方法及び暗号システム、分散デジタル署名システムに関するものである。

【0002】

【従来の技術】通信路によって接続された複数の情報処理装置を含む情報通信システムにおいて、送信された情報が指定された受信装置以外に漏れないこと(情報の秘匿)を補償するための技術の1つとして、暗号技術が知られている。暗号技術は、上述のような情報の秘匿機能の他に、受け取った情報が指示された装置から発振されたことや途中で改ざんされなかったことを確認できる認証機能、及びその受けとった情報が指示された装置から発信されたことを第三者にも照明できるデジタル署名と言われる機能を実現するために有効であることもよく知られている。

【0003】特に、公開鍵暗号方式の1つであるRSA暗号を用いて認証及びデジタル署名方式(R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem", Communic

ations of the ACM, 21, 2, 1978, pp. 120-126) は広く知られている。通常、上述の認証機能は2つの手順によって構成される。一方は送信側が送信情報に対して独自の情報を与える署名であり、他方は受信側が受け取った情報に与えられた送信側の独自情報により、確かにその情報が指示された装置から発信されたことや途中で改ざんされなかったことを確認する認証である。

【0004】また、前述のように守秘及び認証を実現する情報通信システムにおいて、与えられたメッセージのデジタル署名の計算を、通信路によって接続された複数の情報処理装置の間で分散して行う方法が、Yvo desmedt, Yair Frankel ("Threshold cryptosystems", Advances in Cryptology-Crypto'89, 435, Springer-Verlag, 1990, p. 307-315; "Shared generation of Authenticators and Signatures", Advances in Cryptology-Crypto'91, 576, Springer-Verlag, 1992, pp. 457-469) により提案されている(図7)。以下、上記複数の情報処理装置を署名者グループといい、そのグループに参加する各情報処理装置を加入者という。また、そのグループに参加する加入者の数を n で表す。

【0005】図7において、秘密情報(鍵) K から n 個の部分情報が生成され、これらは n の加入者によりそれぞれ秘密に保持される。そして、これらの加入者が保持する K_i ($i = 1, 2, \dots, n$) のうちの一定数以上を合成することにより元の秘密(鍵) K が復元され、グループとしてのデジタル署名を生成することが可能となる。これを分散デジタル署名方式と呼ぶ。デジタル署名を生成するには、その署名生成者固有の秘密(鍵)が必要となる。分散デジタル署名方式の基本的な部分は、複数の加入者からなる情報通信システムにおいて、以下に述べるようにしてその秘密を分散する方式である。

【0006】秘密情報を分散するためには、秘密分散(Secret Sharing; SS)と呼ばれる技術が用いられている。秘密分散は、ある秘密情報 X から k 個の部分情報 X_1, X_2, \dots, X_k を生成し、秘密情報 X を復元するためには t 個以上の部分情報が必要であり、 $t-1$ 個未満の部分情報ではその秘密情報に関するどのような情報も得ることができないというものである。

【0007】このとき、その秘密情報を復元するために必要な部分情報の数 t は、しきい値と呼ばれる。その意味で、この秘密を分散する方式はしきい値スキーム(Threshold Scheme)と呼ばれる。具体的に、A. Shamir("How to Share a Secret", Communications of the ACM, Vol. 22, 11, 1979) によるしきい値スキームは、次のようにして実現される。ある1つの情報を秘密に複数の部分情報に分散するために、定数項が前述の秘密情報となる $t-1$ 次の多項式 $f(x)$ をランダムに選び、 k 個の異なる値に対する多項式の値 $f(i)$ ($i = 1, 2, \dots, k$) を求める。この値 $f(i)$ が前述の部分情報 X_i になる。よって、秘密情報は t 個の部分情報を用いた多項式

補間によって復元できるが、 $t-1$ 以下の部分情報では、秘密情報に関するどのような情報も得ることはできない。

【0008】すなわち、前述のY. Desmedt, T. Frankel による秘密分散方式に基づくRSA暗号を用いた分散型デジタル署名方式は以下の条件を満たしている。

1) 署名者グループに対して与えられたメッセージのデジタル署名を生成するためには、 t 人の加入者の協力があれば十分である。

2) しきい値未満の数($t-1$ 以下)の加入者では、与えられたメッセージのデジタル署名を生成できない。

【0009】

【発明が解決しようとする課題】しかしながら、上述の従来例における分散認証システムでは、グループとして署名する際、そのグループに属するすべての加入者が同等に扱われており、どのような条件においても、グループに与えられたメッセージのデジタル署名を生成する際には、常に一定数以上の加入者の同意が必要であったため、命令系統や地位といった階層構造を有するグループでの利用には適していなかった。

【0010】本発明は、各加入者がデジタル署名生成などに関与できる度合いを階層的に管理することにより、階層構造を有するグループでの利用に適した鍵管理方法及び暗号システム、分散デジタル署名システムを提供するものである。すなわち、本出願に係る第1の発明の目的は、代表者とその他一般の加入者からなる2階層により構成されるグループに適した鍵管理方法及びシステムを実現することである。

【0011】本出願に係る第2の発明の目的は、代表者とその他一般の加入者からなる2階層により構成されるグループに適したデジタル署名システムを実現することである。本出願に係る第3の発明の目的は、代表者とその他一般の加入者からなる2階層により構成されるグループに適した暗号システムを実現することである。

【0012】本出願に係る第4の発明の目的は、さまざまな階層に属する加入者により構成される多階層のグループに適した鍵管理方法及びシステムを実現することである。本出願に係る第5の発明の目的は、さまざまな階層に属する加入者により構成される多階層のグループに適したデジタル署名システムを実現することである。

【0013】本出願に係る第6の発明の目的は、さまざまな階層に属する加入者により構成される多階層のグループに適した暗号システムを実現することである。本出願に係る第7の発明の目的は、さまざまな階層に属する加入者により構成され、かつその中に代表者が存在しないサブグループを有する多階層のグループに適した鍵管理方法及びシステムを実現することである。

【0014】本出願に係る第8の発明の目的は、さまざまな階層に属する加入者により構成され、かつその中に代表者が存在しないサブグループを有する多階層のグル

ープに適したデジタル署名システムを実現することである。本出願に係る第9の発明の目的は、さまざまな階層に属する加入者により構成され、かつその中に代表者が存在しないサブグループを有する多階層のグループに適した暗号システムを実現することである。

【0015】

【課題を解決するための手段】上記目的を達成するため、本発明の鍵管理方法は、通信路によって接続された複数の情報処理装置を含む情報通信システム上で機能する鍵管理方法において、秘密の鍵 K を保持する1個以上の第1の加入者と、元の秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i=1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の加入者とを設け、前記第1の加入者は自分の鍵 K を情報通信システムの鍵とすることができるのに対し、前記第2の加入者は所定数以上の部分情報 K_{1i} を集めてはじめて情報通信システムの鍵とすることを特徴とする。

【0016】ここで、前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j=1, 2, \dots$), K_{3ijn} ($m=1, 2, \dots$), \dots のうちの1個以上を秘密に保持する複数の第3, 第4, \dots の加入者を設け、前記第3, 第4, \dots の加入者は、それぞれ所定数以上の部分情報 K_{2ij} , K_{3ijn} , \dots を集めてはじめて上層加入者の部分情報 K_{1i} , K_{2ij} , \dots とする。また、元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上については、それらを保持する加入者を設けず、最下層の部分情報に付いては、それぞれを保持する全ての加入者を設ける。また、前記情報通信システムは、分散デジタル署名システム及び暗号システムのいずれかである。

【0017】又、本発明の分散デジタル署名システムは、通信路によって接続された複数の情報処理装置を含む分散デジタル署名システムであって、通信路によって接続された、秘密の鍵 K を保持する1個以上の第1の装置と、元の秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i=1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の装置とを設け、前記第1の装置からは自分単独で署名をすることができるのに対し、前記第2の装置は所定数以上の合意があつてはじめて署名をすることができることを特徴とする。

【0018】ここで、前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j=1, 2, \dots$), K_{3ijn} ($m=1, 2, \dots$), \dots のうちの1個以上を秘密に保持する複数の第3, 第4, \dots の装置を設け、前記第3, 第4, \dots の装置は、それぞれ所定数以上の合意があつてはじめて上層装置の意向となる。また、元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上については、それらを保持する装置を設けず、最下層の部分情報については、それぞれを保持する全ての装置を設ける。

【0019】又、本発明の暗号システムは、通信路によって接続された複数の情報処理装置を含む暗号システムであつて、通信路によって接続された、秘密の鍵 K を保持する1個以上の第1の装置と、元の秘密鍵 K を秘密分散することにより生成した部分情報 K_{1i} ($i=1, 2, \dots$)のうち1個以上を秘密に保持する複数の第2の装置とを設け、前記第1の装置では自分単独で暗号化及び復号をすることができるのに対し、前記第2の装置は所定数以上の部分情報 K_{1i} を集めてはじめて暗号化及び復号をすることができることを特徴とする。

【0020】ここで、前記部分情報をさらに秘密分散することによって生成した部分情報 K_{2ij} ($j=1, 2, \dots$), K_{3ijn} ($m=1, 2, \dots$), \dots のうちの1個以上を秘密に保持する複数の第3, 第4, \dots の装置を設け、前記第3, 第4, \dots の装置は、それぞれ所定数以上の部分情報 K_{2ij} , K_{3ijn} , \dots を集めてはじめて上層装置の部分情報 K_{1i} , K_{2ij} , \dots とする。また、元の秘密鍵 K または最下層を除く中間階層の部分情報のうち1個以上については、それらを保持する装置を設けず、最下層の部分情報については、それぞれを保持する全ての装置を設ける。

【0021】

【発明の実施の形態】以下、添付図面に従つて、本発明の鍵管理方法及びシステムの実施の形態を説明する。

＜実施の形態1＞図1は、実施の形態1の分散デジタル署名システムの構成を示すブロック図である。

【0022】図1において、11a～11dで示されたものは情報処理装置、12は通信路、13は通信路で接続された複数の情報処理装置11a～11dを含むグループを示すものである。また、 K_0 は元の秘密鍵であり、 $K_{11} \sim K_{1n}$ は K_0 を秘密分散することにより生成した部分情報である。加入者0は点線で囲まれたグループにおける代表者で元の秘密鍵（グループとしての鍵）を保持しており、加入者11, 12, \dots , 1nはグループ内の一般加入者でありそれぞれ K_{11} , K_{12} , \dots , K_{1n} を保持しており、これらはみな通信路により接続されている。

【0023】該グループにおいて、グループに属する加入者がグループとしてデジタル署名を行おうとした場合、該グループに与えられたあるいはグループ内で保持するメッセージに対して、加入者0は K_0 を用いることにより単独で署名可能であるが、加入者0が不在であるかまたは署名するか否かの選択を一般加入者に委ねた場合には、一般加入者11～1nのうち t_1 以上が合意することにより、部分情報 $K_{11} \sim K_{1n}$ のうち t_1 以上が集まって多項式補間（式1）により元の秘密鍵 K_0 が計算され、該メッセージに対してデジタル署名を行うことが可能となる。

【0024】ただし、元の秘密鍵 K_0 を分散する際に用いた前述のしきい値スキームにおいて定めたしきい値が

t である(しきい値スキームにおいて K_0)を定数項とする $t-1$ 次の多項式を撰んだ)とすると、 t_1 は t よりも大きな値であるものとする。また、(式1)において、 $K_p(i)$ は $K_{11} \sim K_{1n}$ のうちの t_1 以上の部分情報 $K_{1a(b)}$ ($b=1, \dots, t_1; 1 \leq a(b) \leq n$)から任意の異なる t 個を取り出した各部分情報であり、かつしきい値スキームの多項式に $x_{p(i)}$ ($i=1, \dots, t; 1 \leq p(i) \leq n$)を代入して得られた部分情報であるものとする。

【0025】

【数1】

$$K_0 = \sum_{i=1}^t K_p(i) \cdot \prod_{j=1, j \neq i}^t \frac{-x_p(j)}{x_p(i) - x_p(j)}$$

これは、代表者である加入者0は自分の意志をグループの意志とすることができるのに対し、一般の加入者は一定数以上の同意を得てはじめてグループとしての意志とすることができることを示す。

【0026】ただし、加入者 $h i h m \dots$ や部分情報 $K h i j m$ の“ h, i, m, m, \dots ”はそれぞれ、 h が階層を示し、 i は $h i j m \dots$ の上位に位置する階層1の加入者、 j は $h i j m \dots$ の上位に位置する階層2の加入者、 m は $h i j m \dots$ の上位に位置する階層3の加入者を示している。例えば、階層2の加入者でその上位加入者が13であれば23j ($j=1, 2, \dots$)で、その加入者が保持する部分情報は $K 23j$ となり、その中の加入者237の下位加入者であれば337m ($m=1, 2, \dots$)で、その加入者が保持する部分情報は $K 333a$ となる。

【0027】<実施の形態2>図2は実施の形態1の秘密鍵 K を暗号システムにおける復号鍵とした場合の構成を示すものであり、 K_0 がグループの復号機であり、 $K_{11}, K_{12}, \dots, K_{1n}$ が K_0 の部分情報である以外は実施の形態1と同様の構成である。グループ宛に送られた暗号分またはグループの所有データとして暗号化したメッセージに対して、代表者(加入者0)は単独でメッセージの復号が可能であるが、一般加入者 $1 i$ の場合は一定数 t_1 以上が合意し、それぞれが秘密に保持する部分情報 K_{1i} により復号処理を行い、それらの結果を合成することによりはじめてグループの暗号分を復号することが可能となる。 $t_1 - 1$ 以下の一般加入者が集まって暗号分を復号することは不可能である。

【0028】<実施の形態3>図3において、11a~11jは情報処理装置であり、12は通信路であり、13は通信路で接続された複数の情報処理装置11a~11jを含むグループを示す。また、グループの枠内に示された2種類の破線は、グループ内の複数の情報処理装置を含むサブグループ14, 15である。

【0029】 K_0 は、元の秘密鍵(署名鍵)であり、グループの署名鍵としてグループの代表者(加入者0とする)が保持する。 $K_{11} \sim K_{1n}$ は、 K_0 を秘密分散することにより生成した部分情報で、それぞれ加入者0の下位

に位置する加入者(加入者11, 12, ..., 1nとする)が保持しており、 $K_{211}, K_{212}, \dots, K_{21n'}$ は、部分情報 K_{11} を秘密分散することにより生成した部分情報で、それぞれ加入者11の下位に位置する加入者(加入者211, 112, ..., 21n'とする)が保持しており、 $K_{N12 \dots 1}, \dots, K_{N12 \dots n'}$ は、部分情報 K_{212} を q 回($q > 0$)秘密分散することによって得られた部分情報で、それぞれ加入者212の q 段だけ下位の加入者(加入者 $N12 \dots 1, \dots, N12 \dots n'$ とする)が保持する。

【0030】ここに示すグループは、実施の形態1のようなグループを下位の加入者に対して再帰的に設けていくことにより、実施の形態1のグループを多階層化したものであり、加入者0が属する階層を階層0、加入者 $1 i$ ($i=1, 2, \dots$)が属する階層を階層1、...とする。該グループにおいて、加入者がグループとしてデジタル署名を行おうとした場合、該グループに与えられたあるいは該グループ内で保持するメッセージに対して以下の条件で署名可能である。

【0031】1) 加入者0は単独で署名可能
2) 加入者11, 12, ..., 1nはそのうちの一定数 t_1 以上の合意があれば署名可能である。
3) また、加入者11が不在であるか下位加入者211, 212, ..., 21jに署名するか否かの判断を委ねた場合には、加入者211, 212, ..., 21jのうちの一定数 t_2 以上が合意したときに限り、加入者11の代理としてグループの署名に加わることが可能となる。ただし、加入者211, 212, ..., 21jがすべて合意したとしてもグループとして署名することは不可能である。

【0032】4) さらに、下位に位置する階層のサブグループの加入者は、一定数の合意によりそのサブグループの代表者(例えば、図3中の加入者212とその下位の加入者からなるサブグループにおいて、加入者212は該サブグループの代表者となる)の代わりに署名に参加することが可能となる。

<実施の形態4>図4は、実施の形態3において元の秘密鍵 K_0 を暗号の復号鍵とした場合であり、 $K_{11}, K_{12}, \dots, K_{1n}$ が復号鍵 K_0 の部分情報であり、 $K_{211}, K_{212}, \dots, K_{21j}$ が復号鍵の部分情報 K_{11} の部分情報である以外は、実施の形態3と同様の構成である。該グループにおいて、加入者がグループ宛に送られた暗号文またはグループ所有の暗号文を復号しようとした場合、以下の条件で復号可能である。

【0033】1) 加入者0は単独で復号可能
2) 加入者11, 12, ..., 1nはそのうちの一定数 t_1 以上の合意があれば復号可能である。
3) また、加入者11が不在であるか下位加入者211, 212, ..., 21jに復号するか否かの判断を委ねた場合には、加入者211, 212, ..., 21jのうちの

の一定数 t 以上が合意したときに限り、加入者11の代理としてグループの復号に加わることが可能となる。ただし、加入者 $211, 212, \dots, 21j$ がすべて合意したとしてもグループとして復号することは不可能である。

【0034】4)さらに、下位に位置する階層のサブグループの加入者は、一定数の合意によりそのサブグループの代表者の代わりに復号に参加することが可能となる。

<実施の形態5>図5において51は情報処理装置であるが、存在しない場合もあり得る。それ以外の構成は実施の形態3と全く同様である。このような構成をとることにより、実施の形態3を代表者の存在しないグループ13'や、代表者の存在しないサブグループ14'を含むグループに適用することが可能となる。

【0035】例えば、グループの代表者である加入者0が存在しなければ、常にグループ署名の最終決定は、階層1に属する加入者またはサブグループの間で一定数以上の合意を得ることによってなされるし、加入者11が存在しなければ、階層2に属する加入者またはサブグループの間で一定数の合意を得ることによってなされる。

【0036】<実施の形態6>図6は実施の形態5の秘密鍵 K_0 を暗号システムにおける復号鍵とした場合を示すものであり、 K_0 がグループの復号鍵であり、 K_{11}, K_{12}, \dots が K_0 の部分情報、 K_{211}, K_{212}, \dots が K_{11} の部分情報...である以外は、実施の形態5と全く同様の構成である。このような構成をとることにより、実施の形態4を代表者の存在しないグループ13'や、代表者の存在しないサブグループ14'を含むグループに適用することが可能となる。

【0037】例えば、グループの代表者である加入者0が存在しなければ、常にグループの暗号文の復号の最終決定は、階層1に属する加入者またはサブグループの間で一定数以上の合意を得ることによってなされるし、加入者11が存在しなければ、階層2に属する加入者またはサブグループの間で一定数の合意を得ることによってなされる。

【0038】なお、本発明は、複数の機器(例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど)から構成されるシステムに適用しても、一つの機器からなる装置(例えば、複写機、ファクシミリ装置など)に適用してもよい。また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ(またはCPUやMPU)が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【0039】この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現するこ

とになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

【0040】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS(オペレーティングシステム)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0041】さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0042】本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明した処理に対応するプログラムコードを格納することになる。

【0043】

【発明の効果】以上説明したように、本発明によれば、代表者と一般加入者により構成されるグループに適した階層構造の鍵管理方法及び暗号システム、分散デジタル署名システムが構築可能となる。詳細には、秘密分散された鍵を用いる暗号システムにおいて、秘密分散の対象となる鍵 K そのものを保持する加入者(上位加入者)と鍵 K の部分情報 K'_i ($i=1, 2, \dots, n$)を保持する加入者とを設けることにより、鍵 K か、または一定数 t_1 以上の部分情報 K'_i を合成したものの K' ($=K$)のいずれかをグループの鍵として使用可能となる。

【0044】又、暗号システム及び分散デジタル署名システムにおいて、秘密鍵(署名鍵)を本発明の鍵管理システムで管理して、単独で署名可能な上位加入者と一定数の合意なしには署名不可能な下位加入者の2階層を設けることにより、グループの代表者(元の秘密鍵を保持する加入者)の単独でのデジタル署名生成と、グループに属する所定数 t 以上の一般加入者の参加によるデジタル署名生成が可能となる。

【0045】又、鍵 K_0 を保持する加入者と K_0 の部分情報 K_{1i} を保持する加入者の他に、部分情報 K_{1i} を少なくとも一回は秘密分散することによって得られる部分情報 K_{2ij} ($j=1, 2, \dots$), K_{3ijm} ($m=1, 2, \dots$), ...を保持する加入者を設けることにより、所定数以上の部分情報の合成で、その部分情報の元となる部分情報あるいは元の鍵を求めることが可能となる。例え

ば、複数の階層をもつグループがあり、最上位の階層を階層0、次に上位の階層を階層1…とする。このとき階層0には元の秘密鍵を割り当て、階層1には元の鍵の秘密分散することによって生成された部分情報を割り当て、階層2には階層1の部分情報をさらに秘密分散することによって生成された部分情報を割り当て、というように下位の階層になるに従ってより細分化された部分情報が割り当てられているものとする、階層 n に属する任意の部分情報は、それを秘密分散することにより生成された階層 $n+1$ に属する部分情報のうちの所定数 t_{n+1} 以上を合成することにより求めることが可能となる。

【0046】又、暗号システム及び分散デジタル署名システムにおいて、秘密鍵（署名鍵）を上記鍵管理システムで管理して多階層化することにより、グループの代表者（元の秘密鍵を持つ）は単独で暗号化／復号またはデジタル署名を生成でき、所定数 t 以上の一般加入者（秘密鍵の部分情報を持つ）の参加により代表者に代わって暗号化／復号またはデジタル署名を生成可能な他、階層 n のサブグループ（ある部分情報を保持する加入者を代表とし、その部分情報を秘密分散することにより生成された部分情報を保持する加入者により構成されるグループ）に属する一般加入者は所定数 t_{n+1} 以上の参加によりそのサブグループの代表者（上位階層のグループまたはサブグループにおける一般加入者の一人）の代理として暗号化／復号または署名に参加することが可能となる。

【0047】又、鍵管理方法及び暗号システム、分散デジタル署名システムにおいて、最後に秘密分散してできた部分情報以外のうちの少なくとも1個については保持する加入者を設けないことにより、ある部分情報（元の鍵あるいは部分情報の元となる部分情報）を保持する加入者が存在しないサブグループを存在させ、該サブグループにおいては、その部分情報が持つ役割はその下位の階層の属する所定数以上の部分情報の合成によってのみ

実現可能となる。

【0048】以上のように本発明では、複数の加入者からなるグループにおいて、加入者のグループ内での地位に応じて、各加入者に与える署名生成または暗号文復号に関与できる度合いを階層的に分類・管理できる分散署名システムまたは暗号システムを構築することができる。この方式は従来の分散認証システムのように、単に所定数 t 以上の加入者の合意により署名生成や復号処理が可能だけでなく単独での処理が可能な加入者や、所定数 t_n の合意によってある加入者の代理を行うことができる加入者を設けることにより、組織での運用により適した分散認証システムとなっている。

【図面の簡単な説明】

【図1】実施の形態1の分散デジタル署名システムの構成及び鍵管理と認証手続きを説明する図である。

【図2】実施の形態2の暗号システムの構成及び鍵管理と復号手続きを説明する図である。

【図3】実施の形態3の分散デジタル署名システムの構成及び鍵管理と認証手続きを説明する図である。

【図4】実施の形態4の暗号システムの構成及び鍵管理と復号手続きを説明する図である。

【図5】実施の形態5の分散デジタル署名システムの構成及び鍵管理と認証手続きを説明する図である。

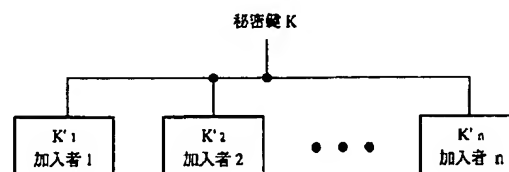
【図6】実施の形態6の暗号システムの構成及び鍵管理と復号手続きを説明する図である。

【図7】従来の分散認証方式における鍵の配送を説明する図である。

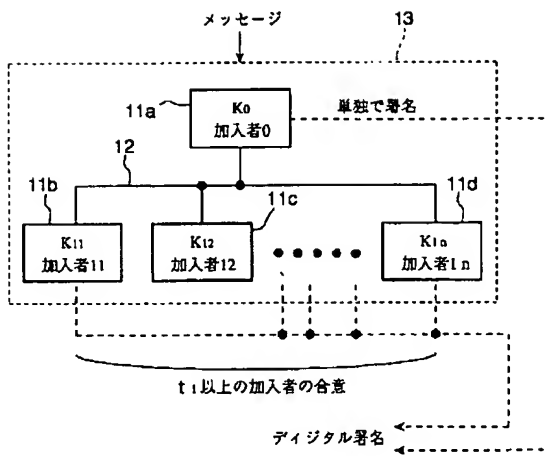
【符号の説明】

- 11 情報処理装置
- 12 通信路
- 13 通信路により接続された複数の情報処理装置を含むグループ
- 14, 15 複数の情報処理装置を含むサブグループ
- 51 情報処理装置

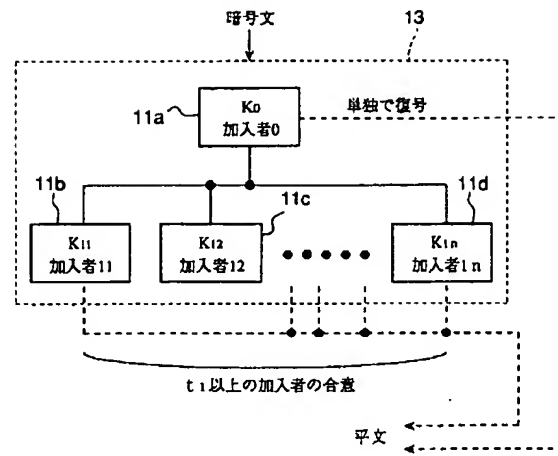
【図7】



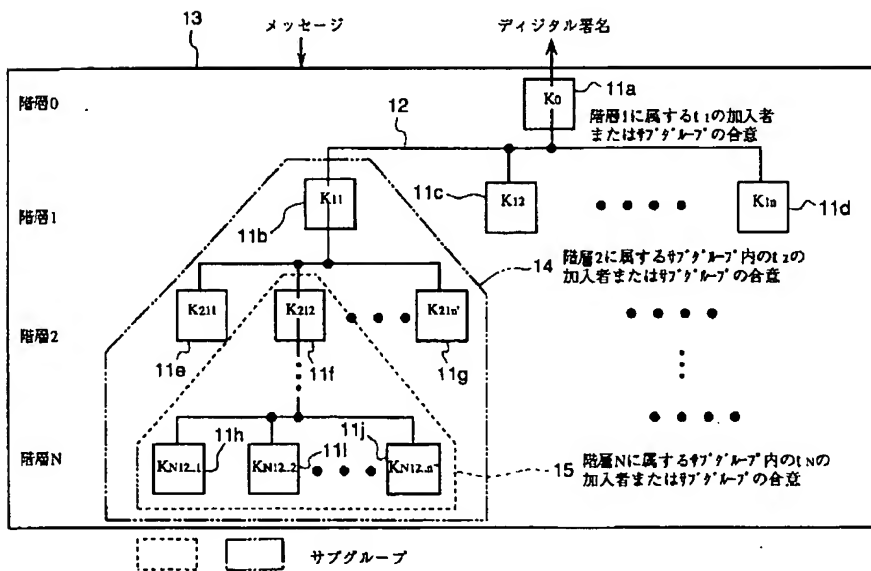
【図1】



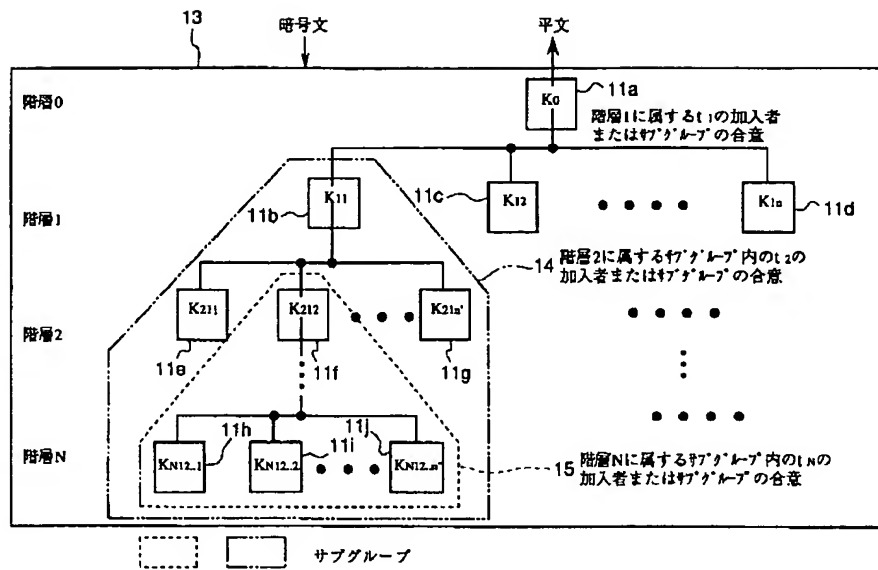
【図2】



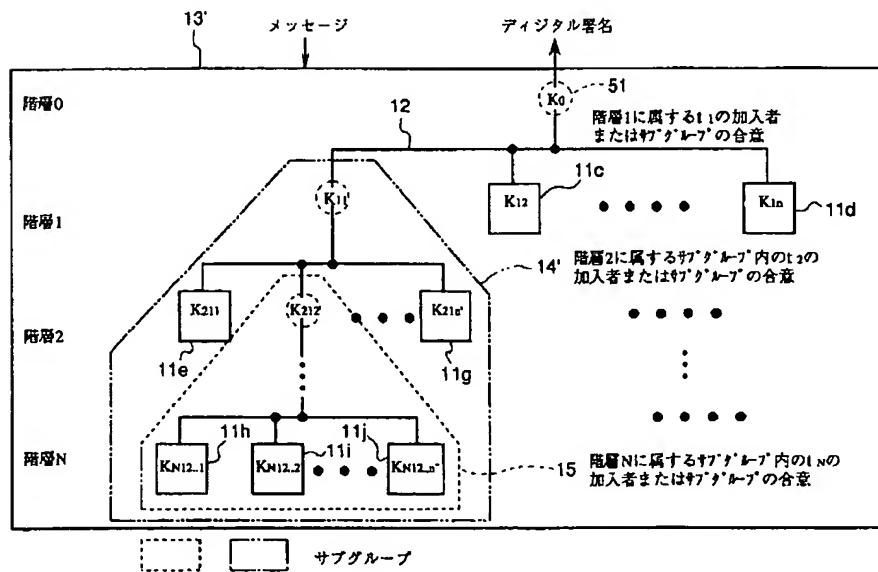
【図3】



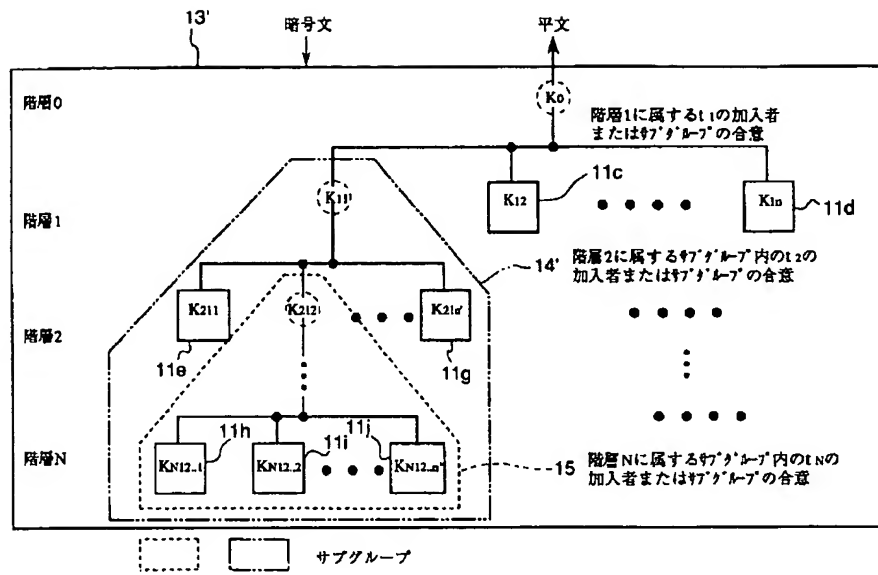
【図4】



【図5】



【図6】



POWERED BY **Dialog**

KEY MANAGING METHOD, CIPHERING SYSTEM, AND DECENTRALIZED DIGITAL SIGNATURE SYSTEM WITH HIERARCHY**Publication Number:** 10-198272 (JP 10198272 A) , July 31, 1998**Inventors:**

- NAGASHIMA TAKAYUKI
- IWAMURA KEIICHI

Applicants

- CANON INC (A Japanese Company or Corporation), JP (Japan)

Application Number: 08-351565 (JP 96351565) , December 27, 1996**International Class (IPC Edition 6):**

- G09C-001/00
- G09C-001/00
- H04L-009/08

JAPIO Class:

- 44.9 (COMMUNICATION--- Other)
- 44.3 (COMMUNICATION--- Telegraphy)

JAPIO Keywords:

- R131 (INFORMATION PROCESSING--- Microcomputers & Microprocessors)
- R138 (APPLIED ELECTRONICS--- Vertical Magnetic & Photomagnetic Recording)

Abstract:

PROBLEM TO BE SOLVED: To provide the key managing method, ciphering system, and decentralized digital signature system which are suitably used by groups with hierarchical structure by hierarchically managing how much respective subscribers can participate in digital signature generation, etc.

SOLUTION: For the key managing method which functions on an information communication system including information processors which are connected by a communication path, ≥ 1 1st subscriber 11a who holds a secret key K and 2nd subscribers 11b to 11d who secretly hold ≥ 1 of pieces of partial information $K(\text{sub } 1i)$ ($i=1, 2, \dots$) generated by decentralizing the original secret key K secretly are provided. While the 1st subscriber can use his or her key K as a key of the information communication system, each 2nd subscriber can obtain a key of the information communication system for the 1st time by gathering more than a specific constant number $t(\text{sub } 1)$ of pieces of partial information K (sub 1i).

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.